JUEGOS ELEMENTALES: FUNCIONES ARITMÉTICAS CLÁSICAS EN CONGRUENCIAS DE NÚMEROS PRIMOS

EDGAR ARMANDO DELGADO VEGA

RESUMEN. Se prueban 8 corolarios de las funciones aritméticas de Euler, Dedekind y Jordan a partir del Teorema de Euler-Fermat para el caso particular de los números primos.
Palabras clave: identidades de funciones aritméticas elementales, congruencias módulo p, funciones aritméticas como potencias.

1. FUNCIONES ARITMÉTICAS CLÁSICAS EN CONGRUENCIAS

Sea p un número primo y $\alpha \in \mathbb{Z}$, $m \geq 2 \in \mathbb{Z}^+$. El teorema modular de la función φ de Euler demuestra que si α y m son primos relativos, entonces

$$\alpha^{\varphi(m)} \equiv 1 \pmod{m}.$$

Así, el teorema de Fermat es un corolario para $m = p$ en el teorema de Euler. Se sabe que $\varphi(p) = p - 1$. En efecto, puede reescribirse como

$$\alpha^{p-1} \equiv 1 \pmod{p} = \alpha^{\varphi(p)} \equiv 1 \pmod{p}.$$

La definición de φ a través de

$$\varphi(m) = m \prod_{p|m} \left(1 - p^{-1}\right),$$

induce la analogía contraria

$$m \prod_{p|m} \left(1 + p^{-1}\right) = \psi(m).$$

La última definición es la función $\psi(m)$ de Dedekind. ¿Qué relación guardan ambas funciones aritméticas? Se plantean dos proposiciones particulares a esta pregunta.

Corolario 1 (Base Dedekind potencia Euler)**.**

$$\psi(p)^{\varphi(p)} \equiv 1 \pmod{p}.$$

Demostración. Por el teorema de Euler. Se debe mostrar que $\psi(p)$ y p son primos relativos. Dado que el único divisor primo de p es sí mismo se deduce la forma de ψ para cualquier primo como $\psi(p) = p\,(1 + 1/p) = p + 1$. Por lo tanto, para cualquier primo se cumple que $(p, \psi(p)) = 1$. □

Corolario 2 (Base Euler potencia Dedekind)**.**

$$\varphi(p)^{\psi(p)} \equiv 1 \pmod{p}.$$

Demostración. El lado izquierdo de la ecuación se reemplaza por $(p-1)^{p+1}$. En consecuencia, el corolario se puede representar como

$$\prod_{j=1}^{p+1} (p-1)_j \equiv 1 \pmod{p} = (p-1)(p-1)\cdots(p-1)_{p-1}(p-1)_p(p-1)_{p+1} \equiv 1 \pmod{p}.$$

Conviene denotar $(p-1) = \alpha \in 2\mathbb{Z}$. En la ecuación, existirán $p-1$ factores lineales α, y dos términos α_p, α_{p+1}. Así, el lado izquierdo se reduce a la expresión $\alpha^{p-1}\alpha^2$. Además, cualquier primo $p \nmid (p-1)^2$. Entonces, la forma de representación lineal para una disposición demostrable por el teorema de Fermat se reescribe

$$(\alpha^2)^{p-1} \equiv 1 \pmod{p},$$

esto finaliza la prueba del corolario. □

Date: 7 de Octubre de 2020.

La función divisor para algún $k \in \mathbb{C}, \sigma_k : \mathbb{N} \to \mathbb{C}$ se define

$$\sigma_k(m) = \sum_{d|m} d^k.$$

Si $m = p$ y $k = 1$, la función divisor se relaciona idénticamente con la función de Dedekind porque p es libre de cuadrados.

Corolario 3 (Relación de Dedekind y Sigma)**.**

$$\sigma_1(p) = \sum_{d|p} d^1 = p \prod_{p|m=p} \left(1 + p^{-1}\right) = \psi(p).$$

Demostración. Para cualquier p, sólo 1 y p son divisores. En consecuencia, la suma de ambos es $p + 1 = \psi(p)$. □

La función de Jordan J_k, es una generalización de la función φ de Euler para potencias k superiores. El caso $k = 1$, es la función φ. Para $k = 2$ aparece representado el producto de φ y ψ.

Corolario 4 (Jordan como producto de Euler, Dedekind y Sigma)**.**

$$J_2(m) = \varphi(m)\psi(m) = \varphi(m)\sigma_1(m).$$

Demostración. Directamente por manipulación algebraica,

$$\varphi(m)\psi(m) = m \prod_{p|m} \left(1 - p^{-1}\right) m \prod_{p|m} \left(1 + p^{-1}\right) = m^2 \prod_{p|m} \left(1^2 - p^{-2}\right) = J_2(m).$$

Esto completa la prueba. □

¿Qué ocurre con la función de Jordan para una base k y un primo p?

Corolario 5 (Jordan para el caso m=p)**.** *Para cualquier* $k \in \mathbb{Z}^+$

$$J_k(p) = p^k - 1.$$

Demostración. Por definición sólo existe un divisor primo de p. Entonces, la forma de Jordan se reduce a $J_k(p) = p^k(1 - \frac{1}{p^k}) = p^k - \frac{p^k}{p^k} = p^k - 1$. □

Luego,

$$J_2(p) = p^2 - 1 \text{ y } J_p(p) = p^p - 1.$$

Una generalización inmediata a la manera de Jordan para una potencia $k = 2$ de la función de Dedekind es

$$\psi_2(m) = m^2 \prod_{p|m} (1 + p^{-2}).$$

Corolario 6 (Identidad de Dedekind generalizada para cualquier base k y m=p)**.**

$$\psi_k(p) = p^k + 1 = \sigma_k(p) = \sum_{d|p} d^k.$$

Demostración. Idéntica a la función de Jordan para $m = p$. □

Luego, $\psi_p(p) = p^p - 1$.

2. Congruencias combinatorias de funciones aritméticas

Se cumplen las relaciones de congruencia módulo p:

$$J_{\varphi p}(p) = p^{p-1} - 1,\ J_{\psi p}(p) = p^{p+1} - 1 \equiv p - 1 \pmod{p}.$$

$$\sum_{d|p} d^{\varphi(p)} = p^{p-1} + 1,\ \sum_{d|p} d^{\psi(p)} = p^{p+1} + 1 \equiv 1 \pmod{p}.$$

Para los productos:

$$J_{\varphi(p)}(p).\sigma_{\varphi(p)}(p) \equiv p - 1 \pmod{p} \quad \text{y} \quad J_{\psi(p)}(p).\sigma_{\psi(p)}(p) \equiv p - 1 \pmod{p}.$$

$$\frac{J_{\varphi(p)}(p)}{\sigma_{\varphi(p)}(p)} \equiv p-1 \pmod{p} \quad \text{y} \quad \frac{J_{\psi(p)}(p)}{\sigma_{\psi(p)}(p)} \equiv p-1 \pmod{p}.$$

$$J_{\varphi(p)}(p).\sigma_{\psi(p)}(p) \equiv p-1 \pmod{p} \quad \text{y} \quad J_{\psi(p)}(p).\sigma_{\varphi(p)}(p) \equiv p-1 \pmod{p}.$$

$$\frac{J_{\varphi(p)}(p)}{\sigma_{\psi(p)}(p)} \equiv p-1 \pmod{p} \quad \text{y} \quad \frac{J_{\psi(p)}(p)}{\sigma_{\varphi(p)}(p)} \equiv p-1 \pmod{p}.$$

Las raíces con índice de alguna función se comportan evidentemente en la forma

$$\sqrt[\varphi(p)]{J_{\varphi(p)}(p).\sigma_{\varphi(p)}(p)} \equiv 1 \pmod{p} \quad \text{y} \quad \sqrt[\psi(p)]{J_{\psi(p)}(p).\sigma_{\psi(p)}(p)} \equiv p-1 \pmod{p}.$$

3. Extensiones de funciones para congruencias

¿Las congruencias se extienden también a las funciones generalizadas?

Corolario 7. $J_2(p)^{\varphi(p)} \equiv 1 \pmod{p}$ y $\left(\sum_{d|p} d^2\right)^{\varphi(p)} \equiv 1 \pmod{p}$.

Demostración. Tanto $(p^2-1,p)=1$ y $(p^2+1,p)=1$. Estas condiciones permiten usar el teorema de Euler. □

El caso anterior se demostró directamente. ¿Sucede lo mismo si la potencia en la congruencia es la función de Jordan?

Corolario 8. $J_2(p)^{J_2(p)} \equiv 1 \pmod{p}$ y $\left(\sum_{d|p} d^2\right)^{J_2(p)} \equiv 1 \pmod{p}$.

Demostración. Por el corolario del producto, $J_2(p)^{J_2(p)}$ puede descomponerse convenientemente en

$$J_2(p)^{\psi(p)\varphi(p)}.$$

Como $J_2(p)=p^2-1=m$ es primo relativo con p, cualquier potencia de m no tendrá a p entre sus factores. Entonces $\left(m^{\psi(p)},p\right)=1$. Luego,

$$\left(J_2(p)^{\psi(p)}\right)^{\varphi(p)} \equiv 1 \pmod{p}.$$

La prueba para $\sigma_2(p)$ es idéntica. □

4. Primos separados en las congruencias con funciones aritméticas

Sean p_m y p_{m+2} primos separados por una distancia de dos. Se cumple la igualdad para congruencias,

Corolario 9.

$$J_2(p_m)^{J_2(p_m)} \equiv 1 \pmod{p_m} \quad \text{y} \quad J_2(p_m)^{J_2(p_m)} \equiv 1 \pmod{p_{m+2}}.$$

$$\left(\sum_{d|p_m} d^2\right)^{J_2(p_m)} \equiv 1 \pmod{p_m} \quad \text{y} \quad \left(\sum_{d|p_m} d^2\right)^{J_2(p_m)} \equiv 1 \pmod{p_{m+2}}$$

Tómese como ejemplo los primos gemelos 3581 y 3583, la fórmula verifica que $J_2(3581)^{J_2(3581)} \equiv 1 \pmod{p} = 12823560^{12823560} \equiv 1 \pmod{3581, 3583}$.